Jurnal Teknologi Sistem Informasi dan Aplikasi **ISSN: 2654-3788**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2654-4229**
Vol. 7, No. 4, Oktober 2024 (1512-1520) **DOI: 10.32493/jtsi.v7i4.44099**

Managing Information Security Risks in Detecting, Handling, and Preventing Cybersecurity Incidents on Local Government Websites

Syaiful Nurul Anam[1], Didit Suhartono[2], Agus Pramono[3]

[1,2,3] Informatics Study Program, Amikom Purwokerto University, Jl. Letjend Pol. Soemarto No.127, Watumas, Purwanegara, Kec. Purwokerto Utara, Kabupaten Banyumas, Jawa Tengah, Indonesia, 53127
e-mail: [1]anam.swyke@gmail.com

Submitted Date: September 28th, 2024 Reviewed Date: October 28th, 2024
Revised Date: October 31th, 2024 Accepted Date: October 31st, 2024

Abstract

Local government websites are increasingly important for distributing information, providing e-services, and facilitating public engagement. However, digitalization brings cybersecurity challenges that jeopardize the integrity, confidentiality, and availability of information. Cybersecurity incidents pose a serious threat, with risks of data breaches, unauthorized access, and system downtimes affecting the reliability and trustworthiness of public services. To address this problem, this study employs the NIST SP 800-30 framework for information security risk management, focusing on detecting, handling, and preventing cybersecurity incidents. The study involved assessing the maturity level of information security controls to identify any gaps and areas of vulnerability. To enhance the implementation of information security policies, the study also utilized tools such as RM Studio, Kali Linux, and Acunetix Web Vulnerability Scanner, which help in identifying and mitigating potential threats more effectively. The results showed that the maturity level of current information security controls is still below the desired target, revealing a significant gap that needs attention. This indicates that while the method provides a structured approach to identifying and addressing security issues, there are still areas for improvement. By emphasizing systematic improvement and focusing on vulnerable points, the study concludes that adopting a combination of the NIST SP 800-30 framework and ISO 27002 standards, along with clear, documented policies, can enhance cybersecurity resilience, reduce risk, and ultimately protect public services. This approach effectively raises the maturity level of information security controls, although continued efforts are needed to fully meet the targeted security standards.

Keywords: Information Security Risk Management; NIST SP 800-30; Cyber Security; Local Government Website; ISO 27002

1. Introduction

Local government websites serve as essential platforms for distributing information to the public, providing electronic services (e-government), and facilitating citizen participation in government processes. They enable easier and faster access to a range of government services and information (Rama & Keevy, 2023). However, with the advancement of digital technology, major cybersecurity challenges have emerged, threatening the integrity, confidentiality, and availability of information delivered through government websites (Mateus-Coelho, 2023).

Cyberattacks on local government websites are no longer hypothetical threats. Incidents such as hacking, data theft, defacement, and Distributed Denial of Service (DDoS) attacks are becoming increasingly common. Several hacking incidents targeting government websites across different regions demonstrate how system vulnerabilities can be exploited by malicious actors (Sia et al., 2021). The impact of these attacks extends beyond the disruption of public service operations; it also directly affects public trust in the government's ability to protect their data (Choejey et al., 2016) Public trust is one of the main pillars of government legitimacy, and disruptions to this trust can have serious long-term consequences, including reduced public participation and weakened support for government policies (Shaheen & Zolait, 2023).

In this context, the implementation of information security risk management becomes crucial. This risk management involves several systematic stages, including the identification of potential threats, the analysis of existing vulnerabilities, the assessment of risk impact, and the implementation of appropriate security controls (Borky & Bradley, 2019) The importance of this approach lies in understanding that not all risks can be completely eliminated; however, through effective risk management, they can be minimized and controlled (Session & Muller, 2022). The first step in information security risk management is the identification of threats. Cybersecurity threats can originate from both internal and external sources. External threats include hackers seeking to exploit system vulnerabilities to gain unauthorized access, malware designed to damage or steal data, and DDoS attacks intended to render services unavailable to users.

Internal threats, on the other hand, may arise from human error—whether intentional or unintentional—as well as system or hardware failures that can lead to data loss (Laksmiati, 2023). After identifying threats, the next step is to analyze the system's vulnerabilities. Vulnerabilities are weak points that threats can exploit to cause harm. These weaknesses may exist in the system's design, the implementation of security controls, or user awareness of cybersecurity practices (Choejey et al., 2015). The goal of vulnerability analysis is to identify the most vulnerable parts of the system that require additional protection (Bada & Nurse, 2019). Incident handling is a critical component of information security risk management. It involves a swift and coordinated response to address incidents as they occur, aiming to minimize their impact (Alexander, 2020). Local governments should have well-trained incident response teams and clear procedures for incident handling, including reporting, investigation, and recovery processes (Broeders, 2016).

Success in incident handling largely depends on the organization's preparedness for emergency situations, including having data backup and disaster recovery plans in place (Pienta et al., 2020). In addition to incident handling, preventive measures are equally important. Prevention can be achieved through proactive security controls, such as the use of firewalls, data encryption, and two-factor authentication (Savaş & Karataş, 2022). Educating and training government staff on cybersecurity practices are also necessary to mitigate risks related to human error (Sadik et al., 2020).

Effective prevention strategies should not only protect systems from known attacks but also adapt to new and evolving threats (van den Berg & Keymolen, 2017). Although the implementation of information security risk management is vital, it is not without challenges. Local governments often face limitations in resources, including budget, infrastructure, and technical expertise (Williams & Woodward, 2015). Budget constraints can hinder local governments' ability to adopt the latest security technologies or update outdated systems (Shaheen & Zolait, 2023). Additionally, the shortage of cybersecurity experts poses a significant challenge, especially in terms of responding quickly and effectively to incidents (Du & Chintakovid, 2023). Another potential obstacle is internal resistance within the organization. Strict security policies may conflict with staff's comfort or habits, impeding the implementation of security strategies (Shires, 2020). Therefore, it is crucial to foster an information security culture within the organization, where every individual understands and values the importance of protecting data and systems (Dixon Prem Daniel & Sundarraj, 2020)).

In this study, information security risk management follows the NIST SP 800-30 framework developed by the National Institute of Standards and Technology (NIST) (Dawkins & Jacobs, 2023). This framework offers structured and comprehensive guidance for managing information security risks, focusing on risk assessment, mitigation, and continuous monitoring (Borky & Bradley, 2019). The primary goal of implementing this framework is to protect information assets, ensure operational continuity, and minimize potential losses from cybersecurity incidents affecting local government websites (Min et al., 2015).

The NIST SP 800-30 framework was selected for this study due to its effectiveness in identifying, assessing, and mitigating information security risks to an acceptable level for the organization, in this case, local governments.

This framework provides a flexible yet structured approach to managing various types of risks, with detailed guidance on risk assessment, response, and continuous monitoring. It enables

local governments to conduct regular risk evaluations and make informed decisions regarding mitigation efforts.

Once the risk management process has been completed, security controls based on the ISO 27002 standard must be implemented to ensure that the risks have been effectively managed, whether through mitigation, acceptance, or risk transfer. The results of the information security maturity assessment in local governments, using controls derived from ISO 27002, will form the basis for developing standard information security policy recommendations. This policy will cover the protection of information managed by local governments, as well as the information systems and technologies used to support operations and public services. The implementation of NIST SP 800-30 is expected to enhance the cybersecurity resilience of local government websites, reduce the risk of cyberattacks, and safeguard the reputation and integrity of services provided to the public.

2. Methods

A. Research Approach

This research adopts a qualitative approach. According (Rukajat, 2018), qualitative research methods are based on the philosophy of post-positivism and are used to study natural conditions, with the researcher acting as the key instrument. Data sources are selected purposively and through snowball sampling, with data collection techniques using triangulation (combined methods) and inductive data analysis. The results of qualitative research emphasize meaning rather than generalization. In this research, a qualitative approach is used to explore and understand how local governments manage information security risks on their websites, following the NIST SP 800-30 framework.

B. Data Collection

The data collection process for this research was conducted through two main methods:

- Literature Review

  Data were collected through literature studies from various trusted sources, such as books, journal articles, lecture modules, and online resources. The primary references include books discussing information security risk management, particularly those detailing the NIST SP 800-30 method, along with other relevant sources. These references form the basis for understanding and applying risk management principles in the context of cybersecurity for local governments.

- Field Methods

  Interviews: Data were gathered through in-depth interviews with individuals responsible for managing information security in local governments, such as the head of the communications and informatics office or members of the IT team. These interviews aimed to explore information related to the implementation of information security risk management, the challenges faced, and the strategies used to anticipate cybersecurity incidents.

  Observation: Direct observations were made of the information technology infrastructure used by local governments, including hardware, software, networks, and applications. The purpose of these observations was to understand how information security is managed in practice and to identify potential risks that may not have been addressed.

  Results: The combined methods revealed a clear gap between the theoretical security frameworks and practical implementation within local governments. Literature insights indicated an ideal model for security risk management, but field observations and interviews showed resource limitations and infrastructural vulnerabilities. Consequently, this gap suggests that to achieve effective cybersecurity resilience, local governments must adopt a gradual, prioritized approach to enhance their information security maturity.

C. Analysis Techniques

This research is exploratory, focusing on information security risk management within local governments. Data analysis was conducted both descriptively and qualitatively to assess and evaluate existing information security practices. The following analysis techniques were used:

- Information Security Maturity Assessment: This assessment was performed quantitatively through questionnaires filled out by respondents responsible for IT management in local governments. The questionnaire was based on the NIST SP 800-30 and ISO 27002 frameworks, aimed at

evaluating the maturity level of information security risk management.

- Qualitative Analysis: Qualitative data from interviews and observations were analyzed thematically to identify patterns and themes related to information security risk management. The results of this analysis were used to formulate recommendations for information security policies that can be implemented by local governments.
- Use of Microsoft Excel: Data from the maturity assessment were analyzed using Microsoft Excel to manage and interpret results related to technical aspects such as software, hardware, and network infrastructure. The findings will help answer the research questions and provide a foundation for developing information security policies.

D. Research Tools

The research tools used in this study include:

- Interviews: Used to obtain in-depth information about threats, vulnerabilities, likelihood, impact, and risk levels. These interviews are a key tool in the qualitative approach to collect in-depth and relevant data.
- Questionnaire: Used to measure the maturity level of information security. This questionnaire is filled out by IT staff who have the authority and responsibility in managing IT in local governments. The results of this questionnaire will be the basis for conducting a quantitative analysis of the state of information security.
- Respondents: The main respondents in this study are staff responsible for IT management in local governments. They were selected based on their roles and knowledge in information security risk management.
- Data Collection and Analysis: Data obtained from interviews and questionnaires will be collected and analyzed to provide an overview of the current maturity level and compare it with the desired maturity level (target maturity level). This analysis will also be used to develop information security policy recommendations that suit the needs of local governments.

Using this approach, this research aims to provide in-depth insights into information security risk management in local governments, while providing recommendations that can improve security and resilience to cyber threats.

Theory: The research draws on established theories of information security risk management, specifically the NIST SP 800-30 framework, which provides a structured approach to identifying, assessing, and mitigating security risks. This framework guides the study's assessment of information security maturity and helps to pinpoint gaps in existing practices within local government environments. The study also references ISO 27002 standards, which are crucial for establishing clear security controls and procedures.

Design/Plan: The design includes a two-phase approach to data collection and analysis:

a. Phase 1: Literature Review and Preliminary Analysis: This phase involves a comprehensive literature review, examining sources that detail information security frameworks, including NIST SP 800-30 and ISO 27002. The findings here help form a baseline understanding of best practices and define evaluation criteria for risk management maturity.
b. Phase 2: Field Methods and Practical Assessment:
   - Interviews: Conducted with local government IT personnel to understand their experiences, challenges, and current security practices. The interview questions are designed to explore both strategic and operational aspects of cybersecurity, covering topics such as resource allocation, incident response, and user training.
   - Observation: Direct assessments of IT infrastructure (hardware, software, networks) are planned to evaluate on-site security controls and identify any unaddressed risks. Observations are documented using a checklist based on the NIST and ISO standards, ensuring a thorough assessment of critical infrastructure elements.

Analysis and Recommendation Plan:

ISSN: 2654-3788
e-ISSN: 2654-4229
DOI: 10.32493/jtsi.v7i4.44099

a. Gap Analysis: Based on the data collected, the study will conduct a gap analysis to compare current practices against the NIST SP 800-30 and ISO 27002 benchmarks.
b. Prioritized Recommendations: The study will then prioritize recommendations that address the most vulnerable areas, focusing on practical and cost-effective solutions to improve resilience, such as upgrading legacy systems, increasing network segmentation, and implementing regular security training.

Results Expected:

This structured design provides a roadmap for enhancing local government security practices, helping to bridge the gap between theoretical frameworks and practical implementation. By following this plan, the research aims to yield comprehensive insights into current information security gaps and to offer tailored recommendations that strengthen cybersecurity resilience.

3. Results And Discussion

Based on the results of the risk assessment from the previous stage, critical assets requiring attention during the risk mitigation process have been identified. This risk mitigation is divided into two main categories: Adversarial Risk and Non-Adversarial Risk, as outlined in the NIST SP 800-30 Revision 1 framework.

A. Adversarial Risk Mitigation

For adversarial risks, mitigation is handled by management responsible for addressing these risks. The qualitative analysis indicates that local governments face information security risks at a Moderate level. Adversarial risks include external threats such as hacking, Distributed Denial of Service (DDoS) attacks, and malware aimed at exploiting system vulnerabilities.

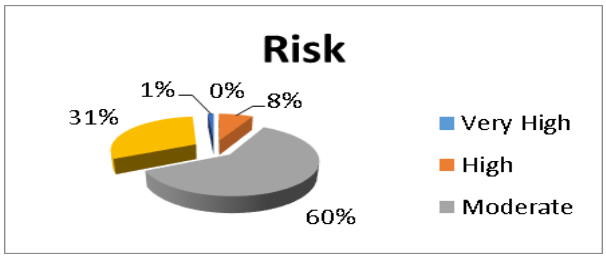

Figure 1. Adversarial Risk Level

Mitigation of these risks involves implementing stronger security controls, such as upgrading firewalls, deploying intrusion detection systems, and enhancing the capacity of incident response teams. The primary focus of this mitigation is to protect the integrity and availability of information managed on local government websites.

B. Non-Adversarial Risk Mitigation

In the Non-Adversarial Risk category, mitigation is directed at internal threats, such as human error, system failure, and other technical issues. The analysis shows that local governments also face non-adversarial risks at a Moderate level.

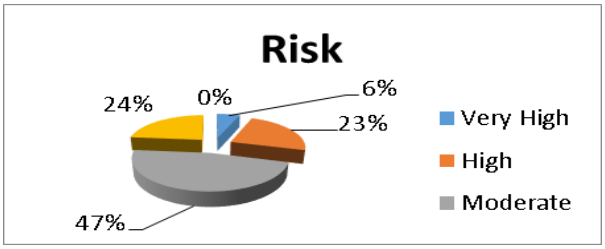

Figure 2. Non-Adversarial Risk Level

To address these risks, mitigation strategies include enhancing staff training on cybersecurity awareness, enforcing stricter system maintenance procedures, and performing regular data backups to minimize the impact of potential system failures.

C. Information Security Maturity Assessment

Before establishing a comprehensive information security policy, an assessment of the local government's current information security maturity level is required. This assessment focuses on the organization’s mission and business processes, particularly those related to information security. In the case study of STMIK Sumedang, this assessment was conducted through qualitative analysis using direct interviews and questionnaires targeted at staff responsible for managing Information Technology (IT) and Information Systems (IS) services.

Based on the results of the information security maturity assessment, which utilized a Score Card developed from the ISO 27002 standard, the following areas were evaluated:

1. Risk Management: The level of risk management regarding information security and the mitigation efforts undertaken.

2. Security Policy: The existence and effectiveness of the implemented information security policy.
3. Organization of Information Security: The structure and responsibilities for managing information security.
4. Asset Management: Identification, classification, and protection of information assets.
5. Human Resource Security: Measures to ensure that staff understand their information security responsibilities.
6. Physical and Environmental Security: Physical protection of IT facilities and infrastructure.
7. Communication and Operations Management: Management of communication and information system operations to ensure service continuity.
8. Access Control: Managing access rights to protect information from unauthorized access.
9. Information Systems Acquisition, Development, and Maintenance: Processes for developing and maintaining secure information systems.
10. Information Security Incident Management: Procedures and responses to information security incidents.
11. Business Continuity Management: Plans to maintain operations during and after incidents.
12. Compliance: Adherence to applicable information security regulations and standards.

The results of this assessment will be used to develop an information security policy tailored to the needs of local governments. The goal of this policy is to enhance cybersecurity resilience, protect reputations, and ensure the continuity of services provided to the public.

By applying the NIST SP 800-30 framework and implementing security controls based on ISO 27002, local governments are expected to improve the maturity of their information security programs, reduce the risk of cyberattacks, and mitigate the impact of potential incidents.

Table 1. Maturity level

ISO Security	Maturity Result	Target Maturity	GAP
Risk Management	3.3	3.5	-0.2
Security Policy	3.7	3.5	0.2
Information Security Organization	3.21	3.5	-0.29
Asset Management	3.45	3.5	-0.05
Human Resource Security	3.7	3.5	0.2
Physical and Environmental Security	3.5	3.5	0
Communication and Operations Management	3.563	3.5	0.063
Access Control	3.553	3.5	0.053
Information Systems Acquisition, Development and Maintenance	3.456	3.5	-0.044
Information Security Incident Management	3.800	3.5	0.300
Business Continuity Management	3.556	3.5	0.056
Compliance	3.625	3.5	0.125

Overall, the data shows that most areas of the organization's information security program are approaching or even exceeding the expected maturity targets. Areas with negative gaps, such as Risk Management and Information Security Organization, require attention to meet the desired targets, while other areas demonstrate maturity levels that are already satisfactory or above expectations.

The small gaps in various areas indicate that the organization is in a strong position but requires some adjustments to achieve or maintain optimal maturity levels.

Maturity is achieved through efforts to address or minimize the gaps identified in the information security controls' maturity levels, based on the NIST SP 800-30 framework. In this context, the implementation of security controls by management on the Local Government Website still shows that the maturity level of some controls is below the expected target.

Therefore, achieving the desired level of maturity requires the following strategic considerations:

1. Gradual Learning Process: Maturity is achieved in stages, with each stage being part of a continuous learning process. Each level of maturity must be implemented to ensure ongoing improvements in managing information security within the Local Government.
2. Improvement Based on Priority Scale: Enhancements should be made incrementally and based on a priority scale. Areas with a lower maturity level should receive higher priority for improvement, enabling the Local Government Website to reach a higher level of maturity in information security management.
3. Learning Towards Maturity Level 3: The learning process aims to achieve Maturity Level 3 within the organization, where information security controls and procedures are consistently implemented and thoroughly documented in accordance with adopted standards

In addition to implementing policy recommendations and improvements, Local Government Website management must implement, document, socialize, and use application tools to optimize the developed information security policies. Some recommended tools for optimizing the implementation of information security policies include:

1. Risk Management Tools: RM Studio is a risk management software that can be used by organizations to implement risk management processes and information security policies.
2. Penetration Testing Tools: Kali Linux is an operating system used to test the security of computer systems, networks, databases, and applications. It is essential for identifying potential security gaps before encountering real threats.
3. Web Vulnerability Scanning: Acunetix Web Vulnerability Scanner This tool scans web applications to identify security holes and vulnerabilities in Local Government websites.
4. Network Security Audit Tools: ZenMap and Wireshark are tools for conducting network security audits. ZenMap aids in detecting vulnerabilities in computer networks, while Wireshark provides in-depth packet analysis for identifying potential network threats.
5. Network Configuration Management: MikroTik RouterOS MikroTik RouterOS is an operating system that enables efficient management of computer networks, with features necessary for maintaining network security in Local Government environments.

Additionally, for risk management and the application of security controls, it is important to use Score Cards developed from ISO 27002 and NIST SP 800-30 Rev1 standards. These Score Cards help in conducting structured assessments, control, and handling procedures for information security. However, the analysis reveals that management in Local Government often responds to threats and incidents reactively, without clear guidelines or standard documentation. This results in uncoordinated and unsustainable responses to threats.

In conclusion, many information security risks, threats, and incidents have not been adequately addressed by management. Therefore, it is crucial for Local Governments to adopt clear and structured information security policy standards to govern the entire process of using and managing information technology. These standards will support the achievement of Maturity Level 3, which requires solid controls and procedures for maintaining information security. The policy should be tailored to the recommendations derived from the maturity assessment that has been conducted.

4. Conclusion

The conclusion should address the research objectives and go beyond simply restating the results and discussion. It should also highlight the prospects for the development of research findings and potential applications for future studies, based on the outcomes. The conclusion should be written in essay form rather than a numerical list.

Based on the research on information security risk management in detecting, handling, and preventing cybersecurity incidents on local government websites using the NIST SP 800-30 framework, several key conclusions can be drawn:

1. Information Security Maturity Level: The analysis of information security maturity reveals that the maturity level of controls implemented on local government websites remains below the expected target. This indicates that, despite efforts to manage information security, significant gaps persist, requiring attention to reach an optimal maturity level.
2. The Importance of a Systematic Approach: The implementation of information security risk management should be carried out systematically and incrementally. Each stage in the maturity process should be part of a continuous learning and improvement cycle, prioritizing areas that are most vulnerable and in need of immediate enhancement.
3. Use of Tools and Standards: The utilization of software tools such as RM Studio, Kali Linux, Acunetix Web Vulnerability Scanner, ZenMap, Wireshark, and MikroTik RouterOS is essential to optimize the application of information security policies. Additionally, the use of Score Cards developed from the ISO 27002 and NIST SP 800-30 Rev1 standards will facilitate more effective and structured risk assessment and management.
4. Need for a Clear Security Policy Standard: A well-defined and structured information security policy is necessary to regulate the use and management of information technology within local government operations. This policy should include comprehensive, documented procedures to ensure all information security processes are conducted consistently and in alignment with best practices.
5. Urgency of Enhancing Controls and Procedures: To reach the target of Maturity Level 3, organizations must improve their information security controls and procedures. This involves creating, implementing, and monitoring security policies based on recognized standards, as well as conducting regular assessments to verify their effectiveness.

Overall, this research underscores the critical need for continuous and comprehensive information security risk management. By adhering to the NIST SP 800-30 framework and adopting the ISO 27002 standard, local governments can strengthen the cybersecurity resilience of their websites, mitigate the risk of cyberattacks, and safeguard the trust and integrity of the public services they provide.

References

Alexander, R. (2020). Using the Latin Square Design Model in the Prioritzation of Network Security Threats: A Quantitative Study. *Journal of Information Security*. https://doi.org/10.4236/jis.2020.112006

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security*. https://doi.org/10.1108/ICS-07-2018-0080

Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering*. https://doi.org/10.1007/978-3-319-95669-5_10

Broeders, D. (2016). The Public Core of the Internet: An international Agenda for Internet Governance. In *The Public Core of the Internet: An international Agenda for Internet Governance*. https://doi.org/10.26530/oapen_610631

Choejey, P., Fung, C. C., Wong, K. W., Murray, D., & Sonam, D. (2015). Cybersecurity challenges for Bhutan. *ECTI-CON 2015 - 2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*. https://doi.org/10.1109/ECTICon.2015.7206975

Choejey, P., Murray, D., & Che Fung, C. (2016). *Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations*. https://doi.org/10.5121/csit.2016.61505

Dawkins, S., & Jacobs, J. (2023). NIST Phish Scale User Guide. *National Institute of Standards and Technology, Gaithersburg, MD, NIST TN*,

2276.

Dixon Prem Daniel, R., & Sundarraj, R. P. (2020). An e-ADR (Elaborated action design research) approach towards game-based learning in cybersecurity incident detection and handling. *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.623

Du, X., & Chintakovid, T. (2023). *A Survey of Cybersecurity Awareness Among Undergraduate Students at Yunnan University of Finance and Economics in China*. https://doi.org/10.2991/978-94-6463-172-2_78

Laksmiati, D. (2023). Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security. *Journal of Computer Networks, Architecture and High Performance Computing*. https://doi.org/10.47709/cnahpc.v5i1.1991

Mateus-Coelho, N. (2023). Editorial - ARIS - Advanced Research on Information Security. *ARIS2 - Advanced Research on Information Systems Security*. https://doi.org/10.56394/aris2.v3i2.33

Min, K. S., Chai, S. W., & Han, M. (2015). An international comparative study on cyber security strategy. *International Journal of Security and Its Applications*. https://doi.org/10.14257/ijsia.2015.9.2.02

Pienta, D., Tams, S., & Thatcher, J. B. (2020). Can trust be trusted in cybersecurity? *Proceedings of the Annual Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2020.522

Rama, P., & Keevy, M. (2023). Public cybersecurity awareness good practices on government-led websites. *International Journal of Research in Business and Social Science (2147- 4478)*. https://doi.org/10.20525/ijrbs.v12i7.2840

Rukajat, A. (2018). *Pendekatan penelitian kuantitatif: quantitative research approach*. Deepublish.

Sadik, S., Ahmed, M., Sikos, L. F., & Najmul Islam, A. K. M. (2020). Toward a sustainable cybersecurity ecosystem. *Computers*. https://doi.org/10.3390/computers9030074

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*. https://doi.org/10.1365/s43439-021-00045-4

Session, W., & Muller, S. R. (2022). Technology Threat Avoidance Factors Affecting Cybersecurity Professionals' Willingness to Share Information. *Proceedings of the International Conference on Research in Management & Technovation*. https://doi.org/10.15439/2022m4720

Shaheen, K., & Zolait, A. H. (2023). The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain. *Information and Computer Security*. https://doi.org/10.1108/ICS-06-2022-0108

Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*. https://doi.org/10.1080/13523260.2019.1670006

Sia, N. C., Hosseinian-Far, A., & Toe, T. T. (2021). Reasons Behind Poor Cybersecurity Readiness of Singapore's Small Organizations: Reveal by Case Studies. In *Advanced Sciences and Technologies for Security Applications*. https://doi.org/10.1007/978-3-030-68534-8_17

van den Berg, B., & Keymolen, E. (2017). Regulating security on the Internet: control versus trust. *International Review of Law, Computers and Technology*. https://doi.org/10.1080/13600869.2017.1298504

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. In *Medical Devices: Evidence and Research*. https://doi.org/10.2147/MDER.S50048